

## METHOD AND SYSTEM FOR FILTERING HOME-NETWORK CONTENT

## FIELD OF THE INVENTION

The present invention relates to a method for filtering and storing information about content, which is available on a network device in a network and a device for filtering and storing information about content, which is available on a network device in a network

5

## BACKGROUND OF THE INVENTION

"Universal Plug and Play (UPnP) is architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. Universal Plug and Play is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces. The UPnP standard is defined in the document "Universal Plug and Play Device Architecture", Version 1.0, Jun. 8, 2000, (c) 1999-2000 Microsoft Corporation.

15

UPnP AV specifications define the interaction model between UPnP AV devices and associated control points. UPnP AV devices include TVs, VCRs, CD/DVD players, set-top boxes, stereo systems, still-image cameras, electronic picture frames, and PCs. The UPnP AV architecture allows devices to support various types of entertainment content such as MPEG2 and MPEG4 for video, JPEG for pictures, and MP3 for audio. It also allows various types of transfer protocols such as HTTP and Real-time Transport Protocol (RTP).

20

UPnP AV specifications define two types of logical devices on the home network: Media Servers and Media Renderers. They also define four "services" hosted by servers and renderers:

25

The Content Directory Service (CDS) enumerates the available "content" (videos, music, pictures, and so forth).

The Connection Manager Service determines how the content can be transferred from the Media Server to the Media Renderer devices.

The AV Transport Service controls the flow of the content (play, stop, pause, seek, etc.).

The Rendering Control Service controls how the content is played (volume/mute, brightness, etc.).

5           The UPnP ContentDirectory Service (CDS) is a standard that allows devices to advertise the content they store on the network. Other devices (so-called Control Points) can send, browse and query actions to the CDS and thus look through the collection, obtaining meta-data about content like title, authors, media type, supported formats and supported DRM systems. Control Points can set up streams to play the content from the CDS on other  
10 devices (for example on a UPnP TV). Typically, to set up a stream, supported formats and DRM systems have to match on source and sink devices.

The meta-data offered by the CDS is used by Control Points to show it to users, and is used for selecting (searching) of particular content. Especially, it can be used to restrict the content shown to the user to that subset, which is really valid in the current  
15 circumstances. For example, content with a format/DRM system that cannot be rendered on a selected/anticipated Renderer might not be shown to the user. Alternatively, control points first allow users to select content, and subsequently select a compatible Renderer.

Experiments with prototypes of CDS in consumer electronics products have shown that browsing through the available information about content by (all) control points  
20 in the home network can put a significant load on all involved devices and on the network. A related problem is that Control Points often show all available content to a user, even content that cannot be used on any other device in the home. This is irritating to the user when he selects that content, only to find out that it is presented in the wrong format or wrong DRM system.

25

## OBJECT AND SUMMARY OF THE INVENTION

It is an object of the present invention to solve the above mentioned problems.

This is obtained by a method of filtering and storing information about content, which is available on a network device in a network, wherein said network further  
30 comprises network rendering devices adapted for rendering content, the method comprises the steps of:

- filtering said information by removing information about content, which cannot be rendered by at least one of said network devices adapted for rendering content,

- storing said filtered information in a database and making said stored information available on the network.

Thereby stored information is obtained, which identifies content being compatible with at least one network rendering device in a network. The stored information could be made available through e.g. a separate interface, protocol, etc. This information can then be selected before trying to initiate a rendering process, and using this information it can be ensured that only possible rendering processes are selected, or that only content, which can be rendered, is made visible to a user trying to activate a rendering process. When the network is a UPnP network, then control points have faster reaction times when they browse the content directory service - the content directory being the stored filtered information. Further, less load on the content directory service, the control point and the network is obtained when the control point browses the content directories. Further, the content presented to the user on the user screen of a control point only comprises content, which can be used.

In an embodiment content which cannot be rendered by a network rendering device comprises content having a file format, which is not compatible with the network rendering devices. Incompatibility between file format of content and the file formats that can be processed by a rendering device is often a reason for a rendering process not being possible.

In an embodiment content, which cannot be rendered by a network rendering device comprises content having a transport protocol, which is not compatible with the network rendering devices.

In an embodiment content, which cannot be rendered by a network rendering device comprises content having a DRM system, which is not supported by any of the network rendering devices.

In a specific embodiment said method of filtering and storing information about content is performed in predefined time intervals. Thereby the stored information is kept updated even if a network rendering device is removed or added, or if a feature of a network rendering device is changed. By performing the update in predefined time intervals, the update process can easily be implemented without requiring "I am here" information from the network rendering devices.

In an embodiment the method of filtering and storing information about content is performed when a new network rendering device enters the network. This ensures

that the filtered information is always updated and in compliance with the current network state, when a network rendering device is entered in the network.

In an embodiment said method of filtering and storing information about content is performed when a network rendering device is removed from the network. This  
5 ensures that the filtered information is always updated and in compliance with the current network state, when a network rendering device is removed.

In an embodiment said method of filtering and storing information about content is performed when a network device has been removed for a predefined time interval. Thereby, if for some reason a network rendering device is shortly removed for maintenance  
10 or because of a network failure, the filtered information is not changed and network load is minimised. Further, "flickering" behaviour of user interfaces on temporary network glitches is avoided.

In an embodiment the network is a UPnP network, and the information about content being available on a network device is the content information stored by an UPnP  
15 content directory service. Especially in an UPnP network the present invention is advantageous, because functionality already exists where a control point checks a content directory using a content directory service. By filtering the content directory service a control point has faster reaction times when it browses the content directory service - the content directory being the stored filtered information. Further, less load on the content directory  
20 service, the control point and the network is obtained when the control point browses the content directories. Further, the content presented to the user on the user screen of a control point only comprises content, which can be used.

In an embodiment the method further comprises storing said removed information about content, which cannot be rendered by at least one of said network devices  
25 adapted for rendering content and making said stored information available on the network. By storing this information it can still be accessed and used for determining necessary upgrades in the network. In a UPnP network a separate content directory service action for browsing hidden content could be added to the CDS. This would allow a control point to explicitly query, which information has been removed by the filter. This can be useful for  
30 control points that want to upgrade the network by e.g. downloading and installing new codecs, adapting security parameters or suggesting the user to buy new network rendering devices. The service could e.g. return additional meta-data fields providing human readable explanations describing why the content is unusable.

The invention further relates to a filtering device adapted for filtering and storing information about content, which is available on a network device in a network, wherein said network further comprises network rendering devices adapted for rendering content, the network device further comprises:

- 5       - means for filtering said information by removing information about content, which cannot be rendered by at least one of said network devices adapted for rendering content,
- means for storing said filtered information in a database and making said stored information available on the network.

10               In an embodiment the filtering device is adapted for filtering and storing information about content, which is available on a network device in a network, wherein said filtering device is comprised in said network device.

              The filtering device for performing the method defined above could e.g. be implemented within the network device comprising the content, or in a separate remote proxy  
15   being connected to the network device comprising the content.

#### BRIEF DESCRIPTION OF THE DRAWINGS

In the following preferred embodiments of the invention will be described referring to the figures, where

20               figure 1 illustrates a network comprising network rendering devices and a network device comprising content, wherein the network device comprises means for filtering and storing information about the content stored on the network device,

              figure 2 illustrates another embodiment of a network comprising rendering devices and a network device comprising content, wherein the network further comprises  
25   means for filtering and storing information about the content stored on the network device,

              figure 3 illustrates the method of filtering and storing information about the content stored on the network device,

              figure 4 illustrates information about content stored on the network device, after having been filtered.

30

#### DESCRIPTION OF PREFERRED EMBODIMENTS

In figure 1 a network is illustrated comprising network rendering devices 101, 103, 105, 107 and a network device 109 comprising content stored in a database 111. The network device 109 is adapted for sharing the content with the network rendering devices

101, 103, 105, 107 through network connections 110, 113, 115 between the network rendering devices and the network device 109. The content in the database 111 could e.g. be video content or audio content, and the media renderers 101, 103, 105, 107 could be devices adapted for playing back the content such as a TV, videos, DVD, HIFI systems, etc. Due to incompatibility between some of the content in the database 111 and some of the network rendering devices 101, 103, 105, 107 and some of the content in the database 111 might not be compatible with any of the network rendering devices 101, 103, 105, 107. Incompatibility could e.g. be due to:

- 10       - The content format of the content in the database 111 is not supported by the network rendering device 101, 103, 105, 107.
- The network rendering device does not support a DRM (Digital Right Management) system, which matches the content in database 111.
- 15       - The network connection through which DRM protected content in the database 111 is transferred to the network rendering device 101, 103, 105, 107 is not allowed by the content specific DRM system (e.g. due to security issues, such as lack of firewall or wrongly configured firewall).
- The network connection to an external content provider services is currently not functional. This is especially relevant if the content is not stored locally in a home network, but stored on an Internet server and proxied in the home.

20               According to the present invention the network device 109 comprises detection means 117 for identifying network rendering device features such as supported formats, transport protocols and DRM system. Using filtering means 118 this information is compared to the available content in the database 111. Based on this comparison information about available content is filtered and stored in a database also referred to as a content directory, and it is ensured that content, which is offered in the content directory 119 is limited to content being compatible with the connected network rendering devices 101, 103, 105, 107. Different ways of determining incompatibilities could comprise one of the following:

- 30           1. For each piece of content in the database 111, determining all features, which could result in incompatibility, the features comprise information such as content file format, DRM protection of content, etc. For each piece of content checking whether a network rendering device 101, 103, 105, 107 exists, which is not incompatible with the content.

2. For all available content the database 111 determining all features which could result in incompatibility, the features comprising information such as content file formats, different DRM protection systems, etc. For each feature checking whether at least one network rendering device 101, 103, 105, 107 exists, which is not incompatible with the content.

3. Detecting all the features of the content and all the features of the network rendering devices 101, 103, 105, 107 and determining whether the content in the database 111 is compatible with at least one of the network rendering devices 101, 103, 105, 107.

In the event that it cannot be determined or there is doubt whether content can be rendered or not by the network rendering devices, the content identification will not be removed when filtering, instead it could e.g. be flagged with a comment such as "questionable if it can be rendered".

In all the examples a content directory 119 is obtained identifying only the subpart of the pieces of content in database 111 being compatible with at least one of the connected network rendering devices 101, 103, 105, 107.

The compatibility check should be performed periodically to ensure that the content identified in the content directory 119 is kept updated when the network state changes, either because the features of the network rendering devices change (new file formats are supported by a network rendering device because of a software update at the network rendering device) or because a network rendering device is added or removed from the network. In figure 1 an example is illustrated where a network rendering device 107 is removed from the network, then the content identified in the content directory 119, which was only supported by the network rendering device 107 is no longer compatible with any of the network rendering devices 101, 103, 105, 107, and the identified content in the content directory 119 should be updated by removing relevant content identifications.

In figure 2 another embodiment of a network is illustrated comprising network rendering devices 201, 203, 205 and a remote network device 207 comprising a database 209 with content. In this embodiment the device 211 acts as a proxy for remote content 209 stored in a remote network device 207. The remote proxy 211 is adapted for sharing the content 209 with the network rendering devices 201, 203, 205 through network connections 217, 219, 221 between the network rendering devices and the remote network device 207. This example has similar functionality as the example described using figure 1, and the remote proxy 211 functions similar to the network device 109, where detection means 213

for identifying renderer features are comprised in the remote proxy 211 together with the filtering means 214. In this example information about content is retrieved from the remote device 207 using a network connection 223. The generated content directory 215 is illustrated as stored in the remote proxy 211, but alternatively the remote proxy 211 could remotely  
5 store the content directory 215 in the remote device 207.

A possible embodiment of the invention is a network device, which contains a content storage medium like a hard-disk and can be connected to a network, for example using wired Ethernet 802.3. This device implements the UPnP MediaServer functionality to share part of the stored content with other devices on the network. In addition, the device  
10 implements UPnP control point functionality

In figure 3 a method is illustrated according to the above embodiment for filtering and storing information about content according to the present invention being used in an UPnP network. The method is divided by a dotted line 301 in an initialisation phase (above the dotted line) and an updating phase (below the dotted line).

15 Initially in 303 all network rendering devices are discovered using the UPnP-defined SSDP protocol. Then, in 305 for each discovered network rendering device the features are determined by query all supported file formats & transport protocols (e.g. by using the ConnectionManager::GetProtocolInfo() action of the Connection manager of the discovered network rendering device).

20 Next, in 307 the filtered information is determined according to the following rules:

- a. Content A that is available in media formats M1..Mn is not shared if no network rendering device supported one of these formats in the last X seconds [where X is configurable].
- 25 b. Content A that is available on transport protocols T1..Tk is not shared if no network rendering device supported one of these formats in the last X seconds [where X is configurable].

Now the filtered information has been stored, and the update phase is started, the update phase comprises three parallel processes 309, 311 and 313 where the network is  
30 monitored for changes.

In 309 the network is monitored for feature changes e.g. caused by updates of the existing network rendering devices, whereby it can support new file formats or new transport protocols. When a change is detected, then the method returns to 305 where the type of change is determined and to 307 where the filtered information is determined. In



UPnP a transport protocol change could be by discovered by a change in the state variable sinkProtocolInfo.

In 311 the network is monitored for changes related to new network rendering devices entering the network, this could in UPnP network e.g. be discovered if an SSDP  
5 Announce message is received of a new rendering device. When a change is detected then the method returns to 305 where the type of change is determined and to 307 where the filtered information is determined.

In 313 the network is monitored for changes related to new network rendering devices by periodically (in specified time intervals) performing a search. This could e.g. be  
10 performed in UPnP by performing an SSDP M-SEARCH to check for new rendering devices that failed to successfully send an SSDP Announce message on joining the network. When a change is detected, then the method returns to 305 where the type of change is determined and to 307 where the filtered information is determined.

In figure 4 the content of the filtered information is illustrated. The content A,  
15 B, C, D, E, F, G, H, I, J are stored in the database 401 on a network device in a network. The network further comprises the network rendering devices 403, 405, 407. The detection means 409 identifies network rendering device features and using filtering means 411 this information is compared to the available content in the database 401. Based on this comparison, information about available content in the database 401 is filtered and stored in a  
20 database also referred to as a content directory 413, and it is ensured that content, which is offered in the content directory 413 is limited to content being compatible with the connected network rendering devices 403, 405, 407 - in this case only content F, I, and J.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative  
25 embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word 'comprising' does not exclude the presence of other elements or steps than those listed in a claim. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device claim  
30 enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.